International Journal of Advanced Computer Technology (IJACT)
ISSN: 2319-7900 Volume VIII, Issue V, October 2019

Survey on Reversible Data Hiding in Encrypted Images Using POB Histogram Method

Sweta Kapse[1], Department of CSE, TITS, RGPV, Bhopal, India; [1]swetakapse15693@gmail.com;
Kedar Nath Singh[2], Department of CSE, TITS, RGPV, Bhopal, India; [2]cseknsingh@gmail.com;

Abstract— *this paper describes a survey on reversible data hiding in encrypted images. Data hiding is a process to embed useful data into cover media. Data invisibility is its major requirement. Data hiding can be done in audio, video, image, text, and picture. Here use an image for data hiding especially digital images and existing method (Histogram Block Shift Base Method) HBSBM or POB. Now a day's reversible data hiding in encrypted images is in use due to its excellent property which is original cover image can be recovered with no loss after extraction of the embedded data. Also, it protects the original data. According to the level and kind of application one or more data hiding methods is used. Data hiding can be done in audio, video, text, and image and other forms of information. Some data hiding techniques emphasize on digital image security, some on the robustness of digital image hiding process while other's main focus is on imperceptibility of a digital image. The capacity of digital information which has to hide is also the main concern in some of the applications. The objective of some of the papers mentioned below is to achieve two or more than two parameters i.e. Security, robustness, imperceptibility and capacity but some of the parameters are trade-off which means only one can be achieved on the cost of other. So the data hiding techniques aiming to achieve maximum requirements i.e. security, robustness, capacity, imperceptibility etc. and which can be utilized in the larger domain of applications is desired. Related work for techniques used for data hiding in a digital image is described in this paper.*

Keywords: - *RHD, Data Hiding, Histogram, Histogram Block Shift Base Method, Mean Square Error, PSNR, Robustness, Digital images.*

I. INTRODUCTION

Nowadays security is considered as the most important factor in any communication systems. In such security systems, issues are integrity, privacy, authentication and no repudiation, which must be handled carefully. Here the security goals are confidentiality, availability and integrity that can be threatened by security attacks. So to protect the original data from such attacks the reversible data hiding techniques are implemented. Reversible data embedding also called as lossless data embedding embeds confidential data into a cover image in a reversible manner. Encryption and data hiding are the two techniques to protect the data [1]. Fundamentally in the instances of data hiding, the spread article will be influenced by some bending and can't be turned around back to the first question, due to some steady contortion has been struck the spreading protest even after the extraction of a concealed message. Reversible data hiding encourages inconceivable plausibility of uses to connect two arrangements of data, in that way that the concealed message have been separated without affecting the spread item. Subsequently, give an extra plausibility to taking care of two distinct data sets. Numerous reversible data hiding plans have been proposed. Tian proposed a distinction expansion data hiding plan, where the distinction and normal estimations of two neighboring pixels are figured and the mystery data to be inserted are annexed to distinction esteem spoke to as a double number. Alattar, Kim et al, and Weng further expanded Tian's work. Ni et al. proposed a plan of utilizing top/zero focuses on the histogram of spatial area images. Fridrich et al proposed a few methods to implant data. The fundamental thought of their work is to pack the chose image highlights for gaining save space. Hong et al. displayed a plan which plays out a movement of the histogram of expectation errors. It utilizes the middle edge locator (MED) to anticipate pixel values. Barton built up a reversible data implanting calculation that depends on data pressure. In this method, compacted data is to be installed in an image. This paper displays a distinction histogram change reversible data hiding calculation. In this proposed method the pixel pair connection helps anticipate a neighborhood image locale on two-dimensional spaces for fulfilling a succession that comprises of distinction sets. Presently by tallying the distinction matches a two-dimensional contrast histogram is created. As the DPM is an injective mapping strategy which is characterized on distinction sets and it is utilized as a part of late histogram-based methods by characteristic augmentation of expansion implanting and moving strategies. So at last by distinction pair mapping) procedure reversible data inserting is actualized [2]. execution the proposed method utilizes two-dimensional distinction histogram and its particular, as contrasted and the routine one-dimensional histogram-based methods which incorporate more pixels for conveying the data furthermore we can diminish the number of moving pixels. In the past writing investigations of implanting position and determination procedures, another pixel pair choice system is proposed for finding the pixel sets in smooth image districts to install the data. Additionally, it is further utilized for upgrading the inserted execution. Enlightened by these concerns mentioned above, we propose a novel RDHEI scheme using a POB number system, which may be viewed as an alternative means of shifting room for embedding or a lossless compression embedding. In our scheme, the content owner partitions the original image into a series of equal-sized non-overlapping blocks, he/she encrypts these non-overlapping blocks by a stream cipher, and the pixels in each block are associated with

the same encryption key. Based on the same block-division strategy, a data hider computes the differences between the rest pixel (unchanged before and after embedding) and the other pixels in each block.

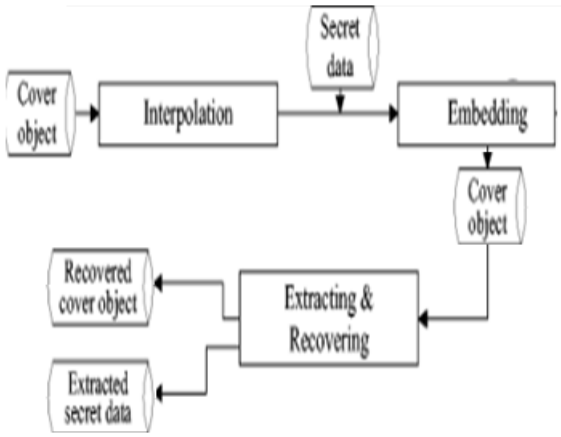

Figure 1 Reversible data embedding and extract process

The functionality, compression synchronized with re-encryption, of POB number is then leveraged to vacate redundancy room for data embedding. This will assist the data hider to embed secret messages into differences ``0'' and ``1'' (two peak points) without any shifting process by using POB-based schemes; in other words, other differences (except ``0'' and ``1'') during the embedding phase remain the same. For the data extraction and image restoration process, the embedded secret messages can be extracted without any error through an accurate calculation of the inverse POB number system, and the image restoration can be implemented perfectly. [3].

Techniques in the first category embed invisible digital data into halftone images, which can be retrieved by scanning and applying some extraction algorithms. These methods include using several different dither cells to create a threshold pattern in the halftoning process, using vector quantization (VQ) to embed watermarks into the most significant bit or least significant bit (MSB/LSB) of error diffusion images using modified data-hiding error diffusion (MDHED) to embed data into error diffusion images, embedding a message into dithering images by using a pair of conjugate halftone screens, using smart pair-toggling (DHSPT) to embed data into error diffusion images, and adopting intensity and connection selection concepts to put the embedded data in a suitable location, coordinating the BCH error-correcting code with data-hiding techniques, and authentication scheme based on halftoning and coordinate projection. Methods in the second category embed hidden visual patterns into two or more halftone images such that it can be perceived directly when the halftone images are overlaid each other. These techniques include using stochastic screen pattern, conjugate halftone screens, and stochastic error diffusion. In, making a different phase version of the stochastic EDF image is adopted to achieve the data-hiding technique. However, the poor contrast of the hidden pattern in the high texture image region was found. For this, we propose an algorithm that is similar in concept to threshold modulation to solve this problem, and the computational complexity is kept relatively low. However, not robust in the printing process is the drawback of the second category.

II. LITERATURE SURVEY

The section describes previous related work under image processing.

M. Naseem et al. [9] in [13] optimized bit plane splicing method is implemented. In this method, the intensity value of the pixel is divided into different planes and rather than using the traditional method of hiding the data into LSB of the pixel and plane by plane, the data in this approach is hidden based on the intensity of the pixels. The pixels are grouped based on the intensity and the number of pixels used to represent the data is chosen depending on the intensities. Also, rather than hiding the data sequentially in the planes, the data is hidden randomly and during the transmission of the data, the planes are transferred randomly to make it difficult to intercept the data. The advantage of this technique is that by grouping the pixels according to the intensity more number of bits is available to represent the hidden data than just the LSB of the pixel

Sandipan Dey et al. [10] to increase and utilize the higher bit planes to hide the data a different approach from the one discussed earlier is employed. This is achieved by converting the original bit planes into some other binary number system using the prime numbers as the weighted function. This enables to use of more number of bits to represent the hidden data.

Das et al [11]. have listed different techniques to hide data The authors have mainly focused on how steganography can be used and combined with cryptography to hide sensitive data. In this approach, they have explained and listed various methods like Plaintext Steganography, Still Imagery Steganography, Audio/Video Steganography and IP Datagram Steganography which can be used to hide data. The authors have also elucidated the Steganalysis process which is used to detect if steganography is used for data hiding**.**

M. Nosrati et al. [12]. In the authors embed the data in RGB 24 bit colour image by using the linked data structures wherein, the data hidden in the image is linked with other data. The advantage of this method is that hiding the data randomly than sequential will make it difficult for the attacker to locate it and also without the authentication key the attacker will not be able to access the next piece of data in the image. Instead of using the whole image as the cover image, the authors have proposed a method that segments the image into blocks of equal sizes. Also, the process involved in this method is reversible hence there is no

loss of hidden data. The approach followed in this scheme to conceal data is quite different. In this technique, the histograms of the blocks of images are taken and they are shifted to the minimum point of the histogram and then the data is hidden between these points. The improvement of this technique is that it provides a higher capacity to hide data than the previous method.

Li et al. et al. [13] in A Modified Reversible Data Hiding in Encrypted Images Using Random Diffusion and Accurate Prediction pointed out this drawback and overcame it by abandoning the idea of block division entirely and using the random diffusion strategy. Besides, accurate prediction is also adopted to improve the fluctuation measurement. In this, the encryption of the host image is achieved by applying a bitwise exclusive-or (XOR) operator to every bit of pixels using an encryption key. The additional messages are embedded into the white set bit by bit. According to the binary value of each bit of the additional message, three LSBs of a series of randomly selected pixels in the white set are simultaneously flipped or not. Thus, the bit is embedded in these pixels. The decryption of the embedded image is similar to image encryption. Afterimage decryption, the unclipped pixels would be equal to the original pixels, and the flipped LSBs of the encrypted pixels in the data embedding phase would be equal to the flipped LSBs of the original pixels. The performance of this method is comparatively better than the previous methods; however, only half of the pixels, i.e. the pixels in the white set, are used for data embedding

M Li et al. [14]. An Improved Reversible Data Hiding for Encrypted Images Using Full Embedding Strategy is an improved version of Li et al.'s method of reversible data hiding of encrypted images is proposed. The previous work partitions the encrypted image into two sets, and only one set is used for data embedding. After carrying out a feasibility analysis, the full embedding strategy is employed in this paper. Accordingly, the data embedding capacity is dilated. In addition to this, the corresponding new fluctuation measurement is designed for the full embedding strategy. The experimental results reveal that the full embedding strategy is effective and also indicate that using the new fluctuation measurement the performance is further increased. This method outperforms other works in terms of performance.

X. Z. et al. [15] in Separable Reversible Data Hiding in Encrypted Image, proposed a novel scheme for separable reversible data hiding in encrypted images. This work solves the problems in the previous paper. Here data can be extracted from the marked encrypted image before image decryption. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data-hider may compress the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional message. With an encrypted image containing an additional message, if a receiver has the data-hiding key, he can extract the additional data though he does not know the image content. If the receiver has the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional message. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in a natural image when the amount of additional message is not too large. This method can apply only for greyscale images.

III EXPECTED OUTCOME

Digital images processing based area data image secure process enhancement in this field find different challenges but identified a better solution and invisible image data. Improve PSNR and minimization MSE.

IV. CONCLUSION

A survey on various reversible data hiding methods to hide and retrieve back in an encrypted image is performed. Some methods embed a large amount of data, some other embed low amount of data. In some techniques data hiding cause distortion to the original image also distort the embedded data. Each method has its positives and negatives. Thus it is necessary to develop an efficient and effective system that provides better security than previous methods. Improve PSNR and minimize error. Focus on a new reversible data compression hiding scheme for hiding message in JPEG image. In this to location map will be compressed to increase the embedding capacity. Comparing with other RDH techniques and literature, this present work often has enhanced flexibility to different images and larger embedding capacity for the same image quality. So the proposed framework has the potential to provide excellent RDH algorithms.

REFERENCES

[1]. S. W. Wang, Y. Zhao, and J. S. Pan, "A Novel Reversible Data Hiding Scheme," International Journal of Innovative Computing, Information and control, vol. 4, no. 2, pp. 351-358, 2008.

[2]. Zhenxing Qian, Xinpeng Zhang and Shuozhong Wang, "Reversible Data Hiding in Encrypted JPEG Bitstream." IEEE Trans. on Multimedia, VOL. 16, NO.5, Apr. 2014.

[3]. W. Hong, T. S. Chen, and C. W. Shiu, " Reversible Data Hiding Based on Histogram Shifting of Prediction Errors," in Intelligent On formation Technology Application Workshops, pp. 292-295, 2008.

[4]. J.M. Barton, "Method and Apparatus for Embedding Authentication Information Within Digital Data," U. S. Patent 5646997, 1997.

[5]. A. M. Alattar, "Reversible Watermark Using the Difference Expansion of a generalized Integer

Transform, IEEE Transaction Image processing, VOL. 13, no. 8 pp. 1147-1156, 2004.

[6]. H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H. G. Choo, A Novel Difference Expansion Transform for Reversible Data Embedding, IEEE Transaction Information Forensics and Security, vol. 3, no. 3, pp. 456-465, 2008.

[7]. J. Tian, "Reversible Data Embedding Using a Difference Expansion" IEEE Transaction Circuits Syst. Video Technology VOL. 13, NO.8, Aug. 2003.

[8]. J. Fridrich, M. Goljan, and R. Du, "Lossless data Embedding – New Paradigm in Digital Watermarking," EURASIP J. Application Signal Process., vol. 2002, no. 2, pp. 185-196, Feb 2002.

[9]. M. Naseem, Ibrahim M. Hussain, M. Kamran Khan, Aisha Ajmal, "An Optimum Modified Bit Plane Splicing LSB Algorithm for Secret Data Hiding", International Journal of Computer Applications, Vol. 29, No. 12, 2011. Foundation of Computer Science, New York, USA, pp. 36-43.

[10]. Sandipan Dey, Ajith Abraham, Sugata Sanyal, "An LSB Data Hiding Technique Using Prime Numbers", IEEE Third International Symposium on Information Assurance and Security, Manchester, United Kingdom, IEEE Computer Society Press, USA, 29-31 Aug. 2007, pp.101-106.

[11]. Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay, Sugata Sanyal, "Steganography and Steganalysis: Different Approaches", International Journal of Computers, Information Technology and Engineering (IJCITAE), Vol. 2, No 1, June 2008, Serial Publications, pp. 1-11.

[12]. M. Nosrati, R. Karimi, H. Nosrati, and A. Nosrati, "Embedding stego-text in cover images using linked list concepts and LSB technique", Journal of American Science, Vol. 7, No. 6, 2011, pp. 97-100

[13]. Li, M., Xiao, D., Peng, Z., and Nan, H.: 'A modified reversible data hiding in encrypted images using random diffusion and accurate prediction', ETRI J., 2014, 36, (2), pp. 325–328.

[14]. M. Li, D. Xiao, A. Kulsoom, and Y. Zhang, Improved reversible data hiding for encrypted images using full embedding strategy, Electronics Letters, 51(9): 690-691, 2015.

[15]. X. Zhang, Separable reversible data hiding in an encrypted image, IEEE Transactions Information Forensics and Security, 7(2): 826–832, 2012.